18. (Amended) The machine readable storage medium of claim 15, wherein transmitting the one or more filters further comprises:

identifying attack traffic characteristics of the attack traffic received by an Internet host;

generating one or more filters based on the identified attack traffic characteristics, such that the one or more filters direct the upstream router to drop network traffic matching the attack traffic characteristics;

digitally signing the one or more filters using a digital certificate of the Internet host; and

transmitting the one or more digitally signed filters to the upstream router.

19. (Amended) A machine readable storage medium including program instructions that direct a system to function in a specific manner when executed by a processor, the program instructions comprising:

establishing a security authentication of a downstream device;

once security authentication is established, verifying that one or more filters from the downstream device select only network traffic directed to the downstream device; and

a4

once verified, installing the one or more filters such that network traffic matching the one or more filters is prevented from reaching the downstream device.

20. (Amended) The a machine readable storage medium of claim 19, wherein establishing security authentication further comprises:

receiving a routing protocol update from the downstream device;

selecting authentication information from the received routing protocol update;

authenticating an identity of the downstream device based on the selected authentication information;

once authenticated, selecting the one or more filters from the received routing protocol; and

authenticating integrity of the one or more filters based on a digital signature of the filters.

21. (Amended) The machine readable storage medium of claim 19, wherein verifying the one or more filters further comprises:

authenticating a source of the one or more filters received as the downstream device;

once authenticated, verifying that a router administrator has set a DDoS squelch time to live value for received filters;

once verified, generating a filter expiration time for each filter based on the time to live, such that the filters are uninstalled once the expiration time expires;

verifying that an action component of each of the filters is drop; and

otherwise, disregarding the one or more filters received from the Internet host.

22. (Amended) The machine readable storage medium of claim 19, wherein verifying the one or more filters further comprises:

selecting a destination address component for each of the one or more filters received from the downstream device;

comparing the destination address components against an address of the downstream device;

verifying that the selected destination addresses matches the downstream device address; and

otherwise, disregarding the one or more filters received from the downstream device.

23. (Amended) The machine readable storage medium of claim 19, wherein establishing security authentication further comprises:

receiving a request for security authentication including authentication information from the downstream device;

selecting the authentication information from the security authentication request; and

a4

authenticating an identity of the downstream device based on the selected authentication information.

24. (Amended) The machine readable storage medium of claim 19, wherein installing the one or more filters further comprises:

selecting network traffic matching one or more of the filters received from the downstream device; and

dropping the selected network traffic such that attack traffic received from one or more attack host computers by the downstream device is eliminated in order to terminate a distributed denial of service attack.

25. (Amended) The machine readable storage medium of claim 19, further comprising:

determining, by an upstream router receiving the one or more filters from the downstream router, one or more ports from which attack traffic matching the one or more received filters is being received;

selecting a port from the one or more determined ports;

determining an upstream router coupled to the selected port based on a routing table;

securely forwarding the one or more received filters to the determined upstream router as a routing protocol update; and

a4

repeating the selecting, determining, and forwarding for each of the one or more determined parts.